RECEIVED
CENTRAL FAX CENTER
FEB 04 2008

REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-25 are pending in the application. The Examiner additionally stated that claims 1-25 are rejected. By this communication, claims 1, 8, 15-16, and 21 are amended. Hence, claims 1-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §102(e)

The Examiner rejected claims 1-6, 8-19, and 21-24 under 35 U.S.C. 102(e) as being anticipated by Kessler, US6789147 (hereinafter, "Kessler"). Applicant respectfully traverses the Examiner's rejections.

Referring to claims 1 and 21, the Examiner noted that Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8). The Examiner noted that this meets the limitation of a fetch logic, disposed within a microprocessor, configured to receive a cryptographic instruction as a part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations.

The Examiner also stated that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of wherein said cryptographic instruction prescribes one of a plurality of cryptographic algorithms, algorithm logic, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to execute said one of the cryptographic operations according to said one of a plurality of cryptographic algorithms.

The Examiner further observed that using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9, lines 28-43), which meets the limitation of execution logic, operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations.

In reply to arguments made by Applicant in Response A, the Examiner noted that although Applicant argued that Kessler does not disclose "fetch logic, disposed within a microprocessor, configured to receive a cryptographic instruction as part of an instruction flow executing on said microprocessor," the argument is not persuasive because the execution units of the co-processor in Kessler include an execution queue that fetches cryptographic instructions (Figure 8) and therefore meets the claim limitation.

Applicant respectfully disagrees with the Examiner and asserts that although Kessler's execution queue fetches something, such a capability does not meet the limitation recited in claim 1. Kessler's execution queue contains primitive security operations placed therein by a microcontroller. Applicant desires to be very clear, and has amended claim 1 to more precisely recite that it is not just any instruction, or primitive security operation, that prescribes the desired cryptographic operation, but rather is an instruction that has been programmed by an application programmer as part of an application program being executed by the microprocessor. Indeed, the application program also includes other instructions that prescribe integer operations as well as the cryptographic operations. To this end, claim 1 is amended to recite that the execution logic has both an integer unit and a cryptography unit. This is because one aspect of the present invention contemplates a general purpose microprocessor that includes a cryptography unit as part of its execution logic.

In addition, Kessler clearly teaches that his device is a coprocessor, and not a microprocessor, thus Kessler does not meet the aforementioned limitation. Applicant respectfully asserts that one skilled in the art will concur that a microprocessor includes

RECEIVED
CENTRAL FAX CENTER
FEB 0 4 2008

an understood set of functions and logic elements. Generally speaking, a microprocessor is understood by those in the art to be programmable digital electronic component that incorporates the functions of a central processing unit (CPU) on a single integrated circuit (IC). The aforementioned aspects of the microprocessor according to the present invention are very adequately disclosed within the instant application to include the ability to fetch and execute instructions that have been provided in an application program, to perform address translation, to load and store variables from/to memory, etc. Kessler's mechanism does not incorporate the functions of a CPU. He specifically teaches that these functions are provided within a host processor.

Claim 1 recites that the cryptographic instruction is intended for execution by a *microprocessor*, and that the microprocessor performs the specified cryptographic operation. As such, a microprocessor differs from a coprocessor, which is understood by those skilled in the art to only supplement the functions of the CPU. Operations performed by a coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption, as has been discussed in the instant application. Coprocessors require the host main processor to fetch the coprocessor instructions and handle all other operations aside from the coprocessor functions. Accordingly, and as Applicant has discussed in the instant application, a microprocessor is not a coprocessor, nor is a coprocessor a microprocessor. Applicant has discussed the existence and disadvantages of present day cryptographic coprocessors, and has provided the present invention to overcome the disadvantages of such.

Applicant has amended claim 1 to specifically recite that the cryptographic instruction directing execution of a cryptographic operation is part of an application program being executed by the microprocessor and which furthermore prescribes integer operations. Such terminology is well understood and appreciated by one of ordinary skill in the art, and it is respectfully submitted that a coprocessor as is disclosed by Kessler cannot be equated with a microprocessor. In summary, among other novel aspects and features, the technique according to the present invention provides a cryptographic instruction that a programmer can employ to directly program cryptographic operations into an application program, where such operations are performed by a microprocessor that provides a cryptography unit within its execution logic. These features can only be provided by a microprocessor and not by a coprocessor.

In addition, the Examiner noted that Applicant argues, "The claim continues to recited how the cryptographic instruction prescribes one of a plurality of cryptographic algorithms and that Kessler does not teach or suggest an instruction that provides for the foregoing limitations," but that the argument is not persuasive because Kessler discloses that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43).

In reply, Applicant notes that amended claim 1 recites that the cryptographic instruction is part of an application program that is being executed by the microprocessor, and as argued above, Kessler's execution queue contains security primitives (i.e.. microcode sequences) which are provided by a microcontroller. Clearly, Kessler does not meet this limitation.

Also, the Examiner responded that Applicant argues, "Although Kessler teaches a coprocessor approach to performing these operations, as the Examiner suggests, such operations are not performed in a microprocessor responsive to a cryptographic instruction that is fetched from memory as part of an instruction flow," but that this argument is not persuasive because Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8).

In response, Applicant agrees that Kessler discloses a coprocessor, and that his coprocessor includes execution units. But Applicant respectfully submits that Kessler's execution units do not include an integer unit, as is present in a general purpose microprocessor. Applicant submits that one skilled in the art immediately appreciates the distinction between a microprocessor and a coprocessor, but to more clearly point out the distinction, Applicant has amended claim 1 to additionally recite an integer unit, which is absent from Kessler's disclosure. This is because Kessler's coprocessor has no need to perform integer operations. These operations in an application program are performed by the disclosed host processor.

The Examiner furthermore noted that Applicant alleges that the employed hardware of Kessler is external to a microprocessor, but that it is the coprocessor of Kessler that is relied upon by the Examiner to meet the claimed microprocessor, and that all employed hardware relied upon is internal to the coprocessor of Kessler (Figure 2).

Applicant responds that the amended limitations of claim 1 now contemplate hardware that is within the host processor disclosed by Kessler and furthermore comprehend an application program that is executed by the recited elements.

To summarize, Kessler teaches a host processor 202 that communicates with a coprocessor 212 over a system bus 210. Input and output data 208-209 along with requests for cryptographic operations 206 are provided in host memory 204. (Figure 2 and associated discussion). Kessler clearly discloses a coprocessor implementation of a cryptography unit, the limitations and disadvantages of which Applicant has noted and summarized in the instant application in paragraph [0019]. Furthermore, Kessler does not even appreciate the problems associated with such a technique, nor does he provide any motivation for one skilled to provide for a cryptography unit within a microprocessor itself, as has been disclosed in the instant application, and which is recited in claim 1..

One skilled will appreciate that the type of configuration proposed by Kessler is cumbersome in that to provide for encryption and/or decryption of data, a host processor must provide for communication with the coprocessor device via some mechanism over the system bus that is very slow compared to the speed at which the processor itself could perform the work, if it were configured as is disclosed in the instant application.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

Claim 21 recites substantially the same limitations as have been argued above as being allowable over Kessler. Accordingly, it is requested that the rejection of claim 21 be withdrawn as well

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

With respect to claims 22-24, these claims depend from claim 21 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 22-24.

As per claim 16, the Examiner noted that Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8), which meets the limitation of a cryptographic unit within a microprocessor, configured to execute one of the cryptographic operations response to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction is fetched from memory by fetch logic in said microprocessor. The Examiner additionally observed that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of an algorithm field, configured to prescribed one of a plurality of cryptographic algorithms to be employed when executing said one of the cryptographic operations. The Examiner noted that using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9, lines 28-43), which meets the limitation of algorithm logic, operatively coupled to said cryptography unit, configured to direct said device to perform said one of the cryptographic operations according to said one of the plurality of cryptographic algorithms.

Applicant respectfully disagrees and directs the Examiner's attention to arguments provided above in traversal of the rejections of claims 1 and 21. More specifically, claim 16, as amended herein, recites, *inter alia,* that the cryptography unit and algorithm logic are both disposed within a microprocessor having in addition an integer unit for performing integer operation, and the cryptographic operation, along with corresponding cryptographic algorithm, is specified by a cryptographic instruction that is fetched from memory as part of an application program that is being executed by the microprocessor.

Since these limitations are not taught, contemplated, or suggested by Kessler, it is requested that the rejection of claim 16 be withdrawn.

With respect to claims 17-19, these claims depend from claim 16 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 16-19.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 7, 20, and 25 under 35 U.S.C. 103(a) as being unpatentable over Kessler, in view of Miller, US6081884. Applicant respectfully traverses the Examiner's rejections and notes that claims 7, 20, and 25 depend from claims 1, 16, and 21, respectively, and add further limitations over that subject matter which has been argued above as being allowable. Accordingly, it is requested that the rejections of claims 7, 20, and 25 be withdrawn.

RECEIVED
CENTRAL FAX CENTER
FEB 0 4 2008

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

By: /Richard K. Huffman/

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

Date: 02/03/2008